

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-148276
(43)Date of publication of application : 26.05.2000

(51)Int.Cl. G06F 1/00
G06F 15/00

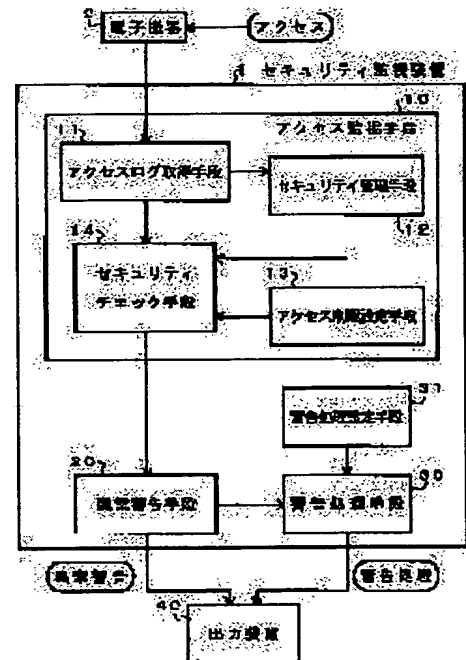
(21)Application number : 10-314134 (71)Applicant : FUJITSU LTD
(22)Date of filing : 05.11.1998 (72)Inventor : SEKIGUCHI MINORU

(54) DEVICE AND METHOD FOR MONITORING SECURITY AND SECURITY MONITORING PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To enable the security monitor device, which monitors access on equipment having an external access means, to maintain and manage the security closely even if user authentication information leaks.

SOLUTION: An access monitor means 10 stores an access log as security management information when access is gained, detects the difference from the obtained security management information from the current access and the past access log to decide whether or not the access is different from normal access, and generates an alarm by an abnormality alarm means 20 if the access is different from the normal access. Further, an alarm processing means 30 once informed of the alarm from the abnormality alarm means 20 performs a specific alarm process set by an alarm process setting means 31.



LEGAL STATUS

[Date of request for examination] 27.08.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-148276

(P 2 0 0 0 - 1 4 8 2 7 6 A)

(43) 公開日 平成12年 5 月 26 日 (2000. 5. 26)

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)
G06F 1/00	370	G06F 1/00	370 E 5B085
15/00	330	15/00	330 A

審査請求 未請求 請求項の数11 O L (全15頁)

(21) 出願番号 特願平10-314134

(22) 出願日 平成10年11月 5 日 (1998. 11. 5)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中 4 丁目 1 番
1 号

(72) 発明者 関口 実

神奈川県川崎市中原区上小田中 4 丁目 1 番
1 号 富士通株式会社内

(74) 代理人 100087848

弁理士 小笠原 吉義 (外 2 名)

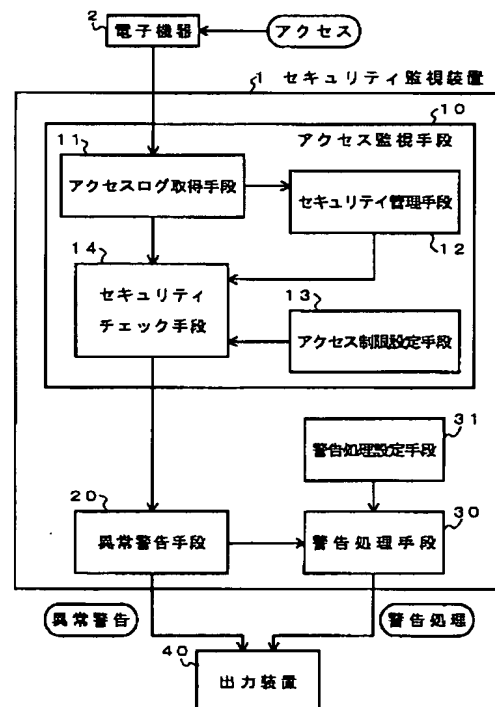
F ターム (参考) 5B085 AC14 AE03 AE06

(54) 【発明の名称】 セキュリティ監視装置、セキュリティ監視方法およびセキュリティ監視用プログラム記録媒体

(57) 【要約】

【課題】 外部からのアクセス手段を有する機器においてアクセスを監視するセキュリティ監視装置に関し、ユーザ認証情報が漏洩したような場合でも、セキュリティの維持管理を強固に行うことができるようにする。

【解決手段】 アクセス監視手段 10 は、アクセスがあった時にアクセスログをセキュリティ管理情報として蓄積し、現在のアクセスと過去のアクセスログから得られたセキュリティ管理情報との差異を検出することにより、通常のアクセスとは異なるアクセスであるかどうかを判別し、通常のアクセスと異なるときは異常警告手段 20 により警告を発する。さらに、警告処理手段 30 は、異常警告手段 20 からの警告通知を受けて、警告処理設定手段 31 によって設定された所定の警告処理を行う。



【特許請求の範囲】

【請求項 1】 電子機器に対する外部からのアクセスを監視するセキュリティ監視装置において、アクセス時のアクセス状況に関するアクセスログを取得するアクセスログ取得手段と、取得したアクセスログを、セキュリティ管理情報として蓄積し管理するセキュリティ管理手段と、前記セキュリティ管理情報に基づいて現在のアクセスが通常のアクセスと異なるアクセスであるかどうかをチェックするセキュリティチェック手段と、現在のアクセスが通常のアクセスと異なるアクセスである場合に警告を発する異常警告手段とを備えることを特徴とするセキュリティ監視装置。

【請求項 2】 請求項 1 記載のセキュリティ監視装置において、前記セキュリティチェック手段は、現在のアクセスのアクセスログと前記セキュリティ管理情報とを比較し、現在のアクセス状況が過去のアクセス状況の範囲に含まれない場合に、通常のアクセスと異なるアクセスであると判断することを特徴とするセキュリティ監視装置。

【請求項 3】 請求項 1 または請求項 2 記載のセキュリティ監視装置において、異常として検出すべきアクセス状況に関する条件を定義するアクセス制限を設定できるアクセス制限設定手段を備え、前記セキュリティチェック手段は、前記アクセス制限設定手段により設定されたアクセス制限に基づいて、警告を発すべき異常アクセスであるかどうかを判断することを特徴とするセキュリティ監視装置。

【請求項 4】 請求項 3 記載のセキュリティ監視装置において、前記アクセス制限設定手段は、セキュリティレベルに応じた複数の設定情報を保持し、前記セキュリティチェック手段は、アクセス状況に応じて変更されるセキュリティレベルに応じて、使用する設定情報を使い分けることを特徴とするセキュリティ監視装置。

【請求項 5】 請求項 1 記載のセキュリティ監視装置において、ユーザからのアクセスに対して前記セキュリティチェック手段により異常アクセスが検出されたとき、そのユーザに第 2 のパスワードを要求し、それが正当と認められる場合にアクセスを許可する警告処理手段を備えることを特徴とするセキュリティ監視装置。

【請求項 6】 請求項 1 記載のセキュリティ監視装置において、前記セキュリティチェック手段により異常アクセスが検出されたとき、そのアクセスをどのように禁止または許可するかを設定できる警告処理設定手段と、前記警告処理設定手段による設定情報に基づいて警告処理を実行する警告処理手段とを備えることを特徴とするセキュリティ監視装置。

【請求項 7】 請求項 1 記載のセキュリティ監視装置において、前記セキュリティ管理手段が管理するセキュリティ管理情報は、ユーザのアクセス時刻に関して統計的に処理したアクセス時間帯の情報を含み、前記セキュリ

ティチェック手段は、前記セキュリティ管理情報におけるアクセス時間帯以外のアクセスに対して異常アクセスと判断することを特徴とするセキュリティ監視装置。

【請求項 8】 請求項 1 記載のセキュリティ監視装置において、前記アクセスは、キーボード、マウス等のコンピュータ等への入力手段を介するもの、機器へのログイン、ファイルへのアクセス、機器を操作するための実行コマンド、またはネットワーク経由のアクセスであることを特徴とするセキュリティ監視装置。

【請求項 9】 監視用入力機器からの入力を監視するセキュリティ監視装置において、前記監視用入力機器により画像または音声情報を入力する画像・音声入力部と、入力した画像・音声のログ情報を、セキュリティ管理情報として蓄積し管理する画像・音声ログ管理手段と、前記セキュリティ管理情報に基づいて、入力された画像または音声情報が通常と異なる画像または音声情報であるかどうかをチェックするセキュリティチェック手段と、入力された画像または音声情報が通常と異なる場合に警告を発する異常警告手段とを備えることを特徴とするセキュリティ監視装置。

【請求項 10】 電子機器に対する外部からのアクセスを監視するセキュリティ監視方法において、アクセス時のアクセス状況に関するアクセスログを取得する過程と、取得したアクセスログを、セキュリティ管理情報として蓄積し管理する過程と、前記セキュリティ管理情報に基づいて現在のアクセスが通常のアクセスと異なるアクセスであるかどうかをチェックする過程と、現在のアクセスが通常のアクセスと異なるアクセスである場合に警告を発する過程とを有することを特徴とするセキュリティ監視方法。

【請求項 11】 電子機器に対する外部からのアクセスを監視するセキュリティ監視方法をコンピュータによって実現するためのプログラムを記録した記録媒体であって、アクセス時のアクセス状況に関するアクセスログを取得する処理と、取得したアクセスログを、セキュリティ管理情報として蓄積し管理する処理と、前記セキュリティ管理情報に基づいて現在のアクセスが通常のアクセスと異なるアクセスであるかどうかをチェックする処理と、現在のアクセスが通常のアクセスと異なるアクセスである場合に警告を発する処理とを、コンピュータに実行させるプログラムを記録したことを特徴とするセキュリティ監視用プログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、電子機器のセキュリティ保護の技術に係り、詳しくは、ユーザに負担をかけることなく複雑な電子機器のセキュリティの維持管理を実現する電子機器のセキュリティ監視装置、セキュリティ監視方法およびセキュリティ監視用プログラム記録媒体に関する。

【0002】

【従来の技術】従来、コンピュータ等の電子機器では、アクセス管理等のセキュリティを維持、管理するために、ユーザIDとパスワードによるユーザ管理方式、暗号化によるデータ漏洩防止方式、アクセス制御方式、認証方式など、さまざまなセキュリティのための監視方式が開発されている。

【0003】このようなセキュリティ監視方式は、主にあらかじめ設定したユーザ等の管理情報（ユーザIDやパスワード等）とユーザが何らかの機器操作をする時点で要求される管理情報とを照合し、それらが規定通りに一致するかまたは許容範囲内にあると認められる場合に、ユーザの要求を実行するものである。すなわち、ユーザの認証に基づくセキュリティ管理を基本としていた。

【0004】

【発明が解決しようとする課題】しかし、このようなユーザIDやパスワード、アクセス制限などのユーザの認証に基づくセキュリティ管理方式では、不正アクセスがあったかどうかを調べるために、常時、そのアクセスログを正規ユーザ自身や管理者が調べ、自分もしくは正規ユーザがアクセスしたものであるかどうかを確認するなどのアクセスログの管理が必要であった。これには、簡単なユーザIDとパスワードではすぐに不正にアクセスされるという根本的欠点があり、ユーザがアクセスログをいちいちチェックしておく必要があって大変面倒であるなどの問題点があった。また、ログ管理を多かれ少なかれ人手に頼っているため、アクセスの正当性の確認に時間がかかり、結果として、不正が発覚するまでに時間がかかっていた。

【0005】また、ユーザ認証情報が漏洩した場合には、不正アクセスがあったかどうかを確認するのに多くの手間と時間がかかるため、不正の発見が遅れるといった問題があった。

【0006】以上のような理由で、ユーザの認証に基づくセキュリティ管理方式は、基本的に認証情報の漏洩に対して、まったくセキュリティ機能が働かないか、またはセキュリティの維持管理にも多くの労力がかかるという欠点があった。

【0007】また、ネットワーク経由のアクセスであって、メールサーバ等のメール受信プロトコルのような基本的にはユーザが介在しない半自動的アクセスは、通常特定ユーザ名を利用して、ある種の特定実行権限をもってほぼ自動的にアクセスしてくるので、セキュリティには十分注意する必要がある。しかし、不正ユーザやウィルス等は、このようなセキュリティの弱点を利用してアクセスしてくる場合が多く、ユーザ認証に基づくセキュリティ監視では、このようなアクセスに対しても基本的に無力である。

【0008】一方、暗号化によるセキュリティ方式で

は、ネットワークを利用したデータ転送時や不正ユーザによるアクセス時に重要な情報が解読されないというようなメリットはあるものの、不正ログインや不正アクセスに対しては無力である。

【0009】本発明の目的は、このようなユーザの認証に基づくセキュリティの維持、管理方式によらず、ユーザやネットワークからのアクセス状況を監視し、通常とは異なるアクセスを検出して警告を発することによって、もしユーザの認証情報が漏洩した場合でも、より強固なセキュリティの維持管理を行うセキュリティ監視方式を提供することにある。

【0010】

【課題を解決するための手段】本発明は、監視対象の電子機器に対する外部からのアクセスを監視し、過去のアクセス状況に関するアクセスログ（セキュリティ管理情報）を参照することにより、新たなアクセスが過去のアクセスログから異常と思われる場合に、何らかの警報を発する機構を持つことをもって主要な特徴とする。

【0011】すなわち、外部からのアクセス手段を有する電子機器において、アクセス時のアクセス環境や時刻などのアクセス状況を取得し、蓄積しておき、そのアクセス状況が所定の基準に該当する場合に、管理者またはユーザに対して何らかの警告を発する。電子機器へのアクセス方法の代表的なものとして、例えばネットワーク、キーボード、マウス等のコンピュータ等への入力手段がある。電子機器へのアクセス内容の代表的なものとしては、例えば機器へのログイン、ファイルへのアクセス、機器を操作するための実行コマンド、ネットワーク経由のアクセスがある。

【0012】また、アクセス状況の基準を、アクセス頻度、アクセス内容（書き込み、読み込み、実行など）に応じて、設定する手段を設けることもできる。例えば過去のアクセスログから得られるセキュリティ管理情報によって、最初のアクセスからある一定回数または一定期間は警告を発するが、何度も同じアクセスを繰り返すと、警告を発しないようにすることができる。

【0013】さらに、あるユーザからのアクセスがあった際に、セキュリティ監視による警告が発せられた後、アクセスをどのように禁止または許可するかを設定する機構を加えることができる。また、パスワードによるセキュリティ管理機構を持つ装置において、あるユーザからのアクセスがあった際に、上記セキュリティ管理情報に基づく警告を発した後、再度、ユーザに対して第2のパスワードを要求し、入力されたパスワードが正当と認められる場合にアクセスを許可する機構を設けることもできる。

【0014】セキュリティ管理情報における時間帯を、ユーザのアクセス時刻に関して正規分布等を用いて統計的に処理し、アクセス時刻の分散値を基準にその警告する範囲を決定することも可能である。

【0015】セキュリティレベルを管理するため、複数のセキュリティ管理情報やアクセス制限情報に関する設定ファイルを利用し、時間経過やアクセス回数などのユーザのアクセス時間経過に応じて、使用する設定ファイルを変更し、セキュリティレベルを変更管理する機構を設けることもできる。これにより、例えば新規ユーザ登録時などに、初期設定したアクセス状況を利用して、新規ユーザに対しては通常ユーザとは異なるセキュリティチェックを適用することができる。

【0016】以上の各処理機構をコンピュータによって実現するためのプログラムは、コンピュータが読み取り可能な可搬媒体メモリ、半導体メモリ、ハードディスクなどの適当な記録媒体に格納することができる。

【0017】

【発明の実施の形態】図1は、本発明の概要を説明するための図である。本発明に係るセキュリティ監視装置1では、コンピュータ等の電子機器2において、アクセス時のアクセス環境や時刻などのアクセス状況を常に監視するアクセス監視手段10と、通常アクセスとは異なるようなアクセスがあった場合に警告を発し、何らかの異常アクセスが発生したことを管理者または特定ユーザに通知する異常警告手段20とを備える。さらに、異常警告手段20による異常警告に伴い、アクセスを一時的に禁止するなどの警告処理設定手段31によって設定された所定の警告処理を実施する警告処理手段30を備える。なお、図1では、電子機器2とセキュリティ監視装置1とを区別して表しているが、セキュリティ監視装置1は、電子機器2の中に組み込まれて電子機器2と一体化したものであってもよい。

【0018】具体的には、電子機器2に対してアクセスがあった場合に、アクセス監視手段10は、アクセスログ取得手段11によりアクセスログを取得し、そのアクセスログを、セキュリティ管理手段12により統計処理して、セキュリティ管理情報として保存する。また、セキュリティチェック手段14により、アクセスログ取得手段11が取得したアクセスログと、過去のアクセスログから得られたセキュリティ管理情報とを比較することによって、今回のアクセス状況と、過去のアクセス状況との差異を検出し、通常とは異なる状況でされたアクセスを異常アクセスと判断し、異常警告手段20により管理者や特定のユーザに警告を発する。

【0019】また、セキュリティチェック手段14によるアクセスログとセキュリティ管理情報との比較において、アクセス制限設定手段13により事前に設定されたアクセス制限を考慮に入れることもできる。今回のアクセスのアクセスログが、設定されたアクセス制限に該当するものである場合には、異常警告手段20により管理者や特定のユーザに警告を発する。さらに、警告処理設定手段31による設定に基づいて、警告処理手段30は、ユーザIDのロック、アクセス禁止、第2パスワード

ドの要求等の警告処理を行う。

【0020】したがって、ユーザ認証情報の漏洩があり、不正ユーザが、正規のユーザとは異なる方法や環境でアクセスを行った場合でも、通常のアクセスと異なる状況でされたアクセス（異常アクセス）として認識し、警告を発することができる。さらに、予め設定しておいた警告処理を直ちに行うことができ、より強固なセキュリティを実現することができる。

【0021】以下、本発明の実施の形態について図面を参照してさらに詳しく説明する。本発明では、原理的には、ユーザの認証情報といったものは不要である。しかし、現在の電子機器ではこのようなセキュリティ管理方法は一般的であり、本発明においても、ユーザの認証情報を利用することによって、より強固なセキュリティレベルを確保できる。したがって、以下に説明する本発明の実施の形態では、従来のユーザ認証に基づくセキュリティ方式に加えて、本発明の方式を用いたものについて説明する。

【0022】〔第1の実施の形態〕まず、第1の実施の形態について説明する。ここでは、コンピュータ等の電子機器に対するアクセスを監視する場合を例にする。

【0023】図2は、本発明の第1の実施の形態についての構成例を示すブロック図である。アクセス監視部110は、監視対象の電子機器に対するアクセスを監視し、ユーザから何らかのアクセスがあると、そのアクセスが通常とは異なるアクセスであるかどうかを検出する。通常どおりのアクセスであれば、そのまま何もせずにアクセス監視が続けられる。しかし、このアクセスが何らかの異常アクセスであると判断されると、異常警告部120に、そのアクセスが異常であることが報告され、異常警告部120は、異常であることを出力装置140を介して特定ユーザまたは管理者に警告する。

【0024】このアクセス監視部110は、電子機器へのアクセスログ201を収集するアクセスログ取得部111、アクセスログ取得部111が収集したアクセスログを統計処理し、セキュリティ管理情報203として管理するセキュリティ管理部112、異常として検出する条件を定義するアクセス制限情報204の設定を行うアクセス制限設定部113、アクセスが異常アクセスであるかどうかをチェックするセキュリティチェック部114から構成される。セキュリティチェック部114は、アクセスログ201とセキュリティ管理情報203との比較により異常アクセスを検出するログ比較部115、アクセスが設定されたアクセス制限情報204の制限にかかるかどうかを比較する制限比較部116からなる。

【0025】アクセスログ取得部111は、アクセスログ201を取得する。機器へのアクセス方法として、他の機器によるネットワークからのアクセス、キーボード、マウス等のコンピュータ等へのさまざまな入力手段からのアクセスがあり、それらのアクセスログを取得す

る。

【0026】図3は、取得されたアクセスログの例を示す図であり、コンピュータへのアクセスについてのアクセスログ201を示す。アクセスログ201として、ユーザ名、パスワード、アクセス日時、アクセスしたファイルのファイル名、実行したコマンドのコマンド名等の情報が収集され記憶される。アクセスログ201は、セキュリティ管理部112に送られる。

【0027】セキュリティ管理部112は、アクセスログ取得部111が取得したアクセスログ201を統計処理し、ユーザごとに、アクセス頻度、アクセス日時の時間帯（何時から何時にアクセスしているか、何曜日にアクセスしているかなど）、過去にアクセスしたファイル名とそのアクセス頻度、アクセスした時間帯、実行したコマンドのコマンド名とその実行頻度、実行した時間帯などのセキュリティ管理情報203に変換して保管する。アクセスログ201は、ファイルごとまたはコンピュータごとに統計処理し、セキュリティ管理情報203として保管してもよい。

【0028】図4は、ユーザに関するセキュリティ管理情報の例を示し、図5はコンピュータに関するセキュリティ管理情報の例を示す。図4のユーザに関するセキュリティ管理情報203は、ユーザごとに保管される情報であり、ユーザのパスワード、アクセス回数、初回および前回のアクセス日時およびアクセス時間帯、アクセスしたファイルごとの初回および前回のアクセス日時、アクセス頻度、アクセス時間帯、実行コマンドごとの初回および前回の実行日時、実行頻度、実行時間帯、アクセスするコンピュータ等の情報である。

【0029】図5のコンピュータに関するセキュリティ管理情報203は、コンピュータごとに保管される情報であり、登録ユーザ名、アクセスしたファイルごとの初回および前回のアクセス日時、アクセス頻度、アクセス時間帯、実行コマンドごとの初回および前回の実行日時、実行頻度、実行時間帯、アクセスするコンピュータまたはアクセスされたコンピュータごとの初回および前回のアクセス日時、アクセス頻度、アクセス時間帯等の情報である。

【0030】図4または図5に示すセキュリティ管理情報203の情報のうち、時間帯の情報に関して、ユーザまたは他のコンピュータがアクセスする時間は、きちんと何時から何時までとは決まっていないし、アクセスを繰り返すうちに徐々にずれてくる場合もある。

【0031】そのため、セキュリティ管理部112では、統計的な処理により、アクセス時間帯の範囲を決定する方法を用いて管理する。例えば、あるユーザのアクセスする時刻を、図6に示すような正規分布と仮定すると、その分布は平均 m と分散 s で表される。したがって、ユーザアクセスを正常と判断する時間帯を $m \pm 3s$ のように分散の $\pm 3s$ の範囲とすれば、あるユーザが過

去にアクセスしてきた時間帯のうち約99.7%の時間帯についてアクセスを無条件で許可するように設定することができる。このようなアクセスに対する統計情報を、過去全部というように区間を区切らずに計算するか、または必要に応じて例えば過去1ヶ月とか1年とかいう区間を区切るかして計算し、それをもとにアクセスを許可する時間帯を設定する。このような方法を用いれば、ユーザのアクセス時間帯が初期設定によらず、ユーザの利用状況によって自動的に変化するので、都合がよい。

【0032】ログ比較部115は、アクセスログ取得部111が取得した今回のアクセスのアクセスログ201と過去に取得したログ情報から得られるセキュリティ管理情報203のアクセス状況を比較する。比較は、セキュリティ管理情報203として保管してある状況のすべてまたは一部について行う。比較する内容は、あらかじめユーザが設定するか、または管理者が決めてもよい。また、所望するセキュリティのレベルに応じて変更してもよい。

【0033】ここで、ユーザuser Aについて、アクセス日時、アクセスファイル、実行コマンドの三種についてセキュリティを管理するものとすれば、それぞれの項目について、今回のアクセスがそのセキュリティ管理情報203の範囲内のアクセスであったかどうかについてログの比較を行い、そのセキュリティ管理情報203の範囲内であれば、通常アクセスであるものとして、次の制限比較部116の処理に移る。

【0034】例えば、アクセスしたファイルの比較では、過去にアクセスしたことのないファイルにアクセスした場合には、セキュリティ管理情報203の範囲外として、警告を発するように異常警告部120に指令を出す。また、実行コマンドの比較では、過去に実行したことのあるコマンドかどうかを比較し、セキュリティ管理情報203に記録のない実行コマンドであれば、警告を発するよう異常警告部120に指令を出す。

【0035】例えば、あるユーザuser Aのアクセスが、図3に示すようなアクセスログ201であり、一方、このユーザuser Aに対して図4に示すようなセキュリティ管理情報203が保存されている場合、ログ比較の結果、このアクセスの時間は18:30:34であるから、セキュリティ管理情報203のアクセス時間帯10:00:00-19:00:00の範囲内となり、ここでは異常なアクセスではないと判断され、さらに制限比較部116により、アクセス制限に該当するかどうかをチェックする処理に進む。

【0036】一方、ユーザuser Aのアクセス時間が21:00:00である場合には、セキュリティ管理情報203の範囲外となるので、ログ比較部115から警告を発することを指示する指令を異常警告部120に出す。

【0037】制限比較部116は、今回のアクセスログ201を、アクセス制限設定部113によって事前に設定したアクセス制限情報204の該当箇所と比較する。比較の結果、アクセスログ201がアクセス制限情報204で設定された範囲外すなわちアクセス可であるならば、警告は発せず、また次のアクセス待ちとなる。一方、アクセスログ201がアクセス制限情報204の範囲内、すなわちアクセス制限にかかる場合には、異常警告部120に対し、このアクセスがアクセス制限にかかった旨の警告指令を出す。

【0038】アクセス制限設定部113は、制限比較部116で用いるための各ファイルや実行コマンドについてのアクセス制限情報204を設定する。図7は、設定されたアクセス制限情報の例を示す。

【0039】アクセス制限情報204は、ファイルへのアクセスまたはコマンドの実行を制限する場合のアクセス頻度、アクセス時間の範囲に関する情報である。例えば、ユーザごとに、アクセスファイル設定として、特定のファイルに対し、「アクセス頻度3以下」、「アクセス時間帯9:00:00-18:00:00以外」というような設定がなされる。また、コマンド実行設定として、特定のコマンドに対し、「実行頻度-1以下」、「実行時間帯0:00:00-0:00:00以外」などのような設定がなされる。

【0040】アクセス制限情報204へのアクセスファイル設定では、ユーザごとに個々のファイルのアクセス可否を設定することにより、ユーザのアクセス管理を行うことができる。例えば管理者のみがアクセスできる管理者ファイルに対して、一般ユーザからのアクセスを制限したい場合、一般ユーザのアクセス制限情報204として、その管理者ファイルへのアクセス制限時間を0:00:00-0:00:00以外のように全時間帯にしておけば、その管理者ファイルへのアクセスを常に許可しないようにすることができる。

【0041】同様に、アクセス制限情報204は、例えばコンピュータのシステム管理用コマンドを一般ユーザに実行させないようにするときにも利用することができる。このような管理用コマンドに対して、アクセス制限情報204のアクセス頻度をアクセス頻度を無限大(図7に示すアクセス制限情報204の例ではマイナスの値で代用している)まで許可しないように設定しておけば、一般ユーザからの管理用コマンドの実行が制限されることになる。

【0042】UNIX系OSなどではファイル属性を変えることによってアクセス管理を行えるが、本方式では、どのユーザがいつどこからアクセスしたか、そのアクセスは通常アクセスなのかそれとも通常とは異なるアクセスなのかというような状況に基づいて、より詳細なファイルアクセスの監視が可能となる。

【0043】異常警告部120は、アクセス監視部11

0から異常であることの報告を受ける異常警告受信部121とその異常警告を受けて実際にどのような警告を発するかを決定し警告を発する警告発信部122からなる。

【0044】異常警告受信部121がアクセス監視部110から異常発生のお知らせを受けると、異常の内容を調べて、どこの誰に警告を発するかを決定し、警告発信部122は、出力装置140を介して警告を発する。警告は、ログ情報として特定のファイルに保存されるようにしてもよいし、システム管理者へメールで送るようにしたり、ディスプレイ等の表示装置に表示するようにしてもよい。

【0045】例えばユーザuser Aに対して図4に示すようなセキュリティ管理情報203が保管されている状態で、図3のアクセスログ201に示すようなアクセスがあったとする。ユーザuser Aに対するアクセス制限情報204としては、図7に示すようなアクセス制限が設定されているとする。ユーザuser Aのファイルfile1.txtへのアクセスは、セキュリティ管理情報203でのアクセス頻度が22であるから、アクセス頻度「3以下」の範囲外であるが、アクセス日時が18:30:34であり、制限時間帯「9:00:00-18:00:00以外」の範囲内となる。したがって、異常なアクセスとして警告が発せられることになる。また、コマンドexec.exeの実行は、セキュリティ管理情報203では実行頻度が62となっているから、実行頻度「3以下」の範囲外であるが、実行日時が18:32:20であり、制限時間帯「9:00:00-18:00:00以外」の範囲内となり、同様に警告が発せられる。

【0046】警告の具体例は、以下のとおりである。ユーザuser Aのアクセス時間が午後9時であった場合には、ユーザuser Aの通常のアクセス時間帯と異なるので、アクセス監視部110から通知を受けた異常警告部120の警告発信部122から、「警告:user Aは異常な時間午後9時にログインしました。」というような警告が、基本的には管理者に対して発せられる。また、ユーザuser Aのアクセスが、過去にアクセスしたことのないファイルに対するものである場合には、「警告:user Aは過去にアクセスしたことのないファイルFにアクセスしました。」というような警告が発せられる。

【0047】ユーザIDとパスワード等によるユーザ認証を行うシステムにおいて、このような状況は、ユーザuser AのIDやパスワード等の認証情報が盗まれたような場合に起こると考えられる。例えば、ユーザuser Aの通常のアクセス時間帯である午前10時から午後7時の間以外の時間にアクセスがあった場合には、通常のアクセス時間帯と違うので、別のユーザがユーザuser AのIDとパスワードを用いてアクセスしている

可能性があり、通常の時間帯でない時間にアクセスがあった旨の警告が発せられる。

【0048】また、コンピュータがネットワーク接続されているような状況においては、あるコンピュータから別のコンピュータに相互ログインすることが多い。このような場合、ユーザが通常どのコンピュータからアクセスしているかをあらかじめ取得しておけば、通常のコンピュータとは別のコンピュータからアクセスしていることを検出した場合に、別のユーザの不正なアクセスである可能性があることから、通常とは違ったコンピュータからアクセスされた旨の警告を発することが可能である。したがって、本方式によれば、ユーザのIDやパスワードが盗まれた場合でも、本来の正規ユーザが使用しないアクセス状況であれば異常なアクセスとして警告が発せられるので、より強固なセキュリティが確保できる。

【0049】図2に示すセキュリティチェック部114においては、説明を簡単にするために、ログ比較部115による異常アクセスの検出と、制限比較部116によるアクセス制限情報204に基づく異常アクセスの検出とが、独立に行われるものとして説明した。しかし、セキュリティチェック部114における異常アクセスの検出を、ログ比較部115による検出と制限比較部116による検出とを関連させた形態で行うようにしてもよい。例えば、所定の設定ファイルに従って、双方で異常と検出した場合にのみ、警告を発するような実施も可能である。また、セキュリティチェック部114を、ログ比較部115または制限比較部116の一方だけで構成することも可能である。ログ比較部115による比較条件を、アクセス制限情報204または他の設定情報に基づいて決定するような実施も可能である。

【0050】以上で説明した方式では、基本的に過去にアクセスしたことがないユーザに関しては、セキュリティ管理情報203に過去のアクセス履歴の蓄積がないことから、常に警告を発することになる。すなわち、新規ユーザは、すべてのアクセスに関して警告が発せられることになり、管理上煩わしいことにもなる。そこで、新規ユーザが警告なしに利用できるように、初期設定として、通常考えられるファイルへのアクセスやアクセス時間帯などを設定した新規ユーザに対するアクセス制限情報を別に用意しておく。こうすれば、このような煩わしい状況を回避することができる。

【0051】また、正規ユーザが正規の方法でアクセスする場合でも、最初は警告を発するが、何度もそのアクセスを繰り返せば、アクセス頻度が上がるので、指定回数以上のアクセス頻度になったら警告しないようにアクセス制限情報を別に設けておけば、所定アクセス回数後のアクセスは、正常なアクセスとして警告を発しなくすることもできる。

【0052】図8は、新規ユーザに対するアクセス制限

情報の例を示す図である。新規ユーザに対するアクセス制限情報205は、新規ユーザや特定のセキュリティレベルのユーザに対して適用する。新規ユーザに対するアクセス制限情報205が適用されるユーザについては、所定期間経過後または所定アクセス回数後、例えば1週間とか3回目のアクセスとかいう時点でセキュリティレベルを通常ユーザ用のセキュリティレベルに変更する。これにより、以後、図8に示す新規ユーザ用のアクセス制限情報205に代わり、図7に示すような通常ユーザに対するアクセス制限情報204が適用される。

【0053】新規ユーザに対するセキュリティレベルと、通常ユーザに対するセキュリティレベルの違いによって、アクセス制限情報を使い分ける例を説明したが、同様にさまざまなセキュリティレベルに対応させたアクセス制限情報を用意することにより、セキュリティレベルを細かく区分して、セキュリティレベルに応じたアクセス監視を実現することもできる。

【0054】また、電子機器へのアクセスとしては、ユーザからのアクセスだけでなく、ネットワーク内の他の機器からの半自動的アクセスもあり得る。例えば、メールサーバなどがそうである。メールは、メールサーバやメールを受信したコンピュータ内のある種のプログラムを起動することができるので、セキュリティの確保が難しい。本方式では、このような基本的にユーザが介在しないコンピュータ同士のアクセスについてもセキュリティの監視が可能である。

【0055】図9は、メールサーバのネットワークを経由するアクセスから得られるアクセスログの例を示す。セキュリティ管理部112は、図9に示すアクセスログ206を、図10に示すようなセキュリティ管理情報207に変換して記憶しておく。

【0056】この場合のログ比較処理は、例えば次のように行われる。ログ比較部115は、図9のアクセスログ206と図10のセキュリティ管理情報207とを比較し、そのアクセスログ206のアクセスが、セキュリティ管理情報207に記録されている既存の送信者からのメールであれば、警告なしに受信する。しかし、セキュリティ管理情報207に記録されていない送信者からのメールである場合には、異常警告部120に異常を通知し、異常警告部120は、例えば次のような警告を発する。

【0057】「警告：未知のユーザからメールが送られてきました。」このような警告を、管理者またはメールの宛先ユーザに対して発することにより、管理者または宛先ユーザは、そのメールを読まずに削除するなり、ウイルスに感染しても構わないコンピュータで読むなりして、任意に処置することができるようになるので、セキュリティの適切な維持・管理が可能となる。

【0058】図11に、第1の実施の形態による処理の流れの概要を示す。アクセスログ取得部111によりア

10

20

30

40

50

クセスログ201を取得し、セキュリティ管理情報203に変換してセキュリティ管理部112に記録する(ステップS1)。次に、ログ比較部115により、アクセスログ201とセキュリティ管理情報203とを比較し(ステップS2)、アクセスログ201の内容がセキュリティ管理情報203の範囲内であるかどうかにより、通常アクセスかどうかを判断する(ステップS3)。通常アクセスでない場合には、ステップS6へ進み、異常警告部120によって異常警告を発する。通常アクセスである場合には、さらに、制限比較部116によりアクセスログ201とアクセス制限情報204とを比較し(ステップS4)、アクセスログ201がアクセス制限の範囲内であるかどうかを判断する(ステップS5)。アクセスログ201がアクセス制限情報204に基づくアクセス制限の範囲内であれば、異常警告部120により異常警告を発し(ステップS6)、アクセスログ201がアクセス制限の範囲外であれば、異常の警告を発することなく、次のアクセスを待つ。

【0059】図1.2は、本発明を適用するもっとも代表的なハードウェアの構成例を示す。この例では、コンピュータ300は、監視対象の電子機器とセキュリティ監視装置100とを兼ねる。コンピュータ300において、ネットワーク304からのアクセスやコンピュータ300本体へのキーボードやマウスなどの入力装置301からのアクセスが監視され、警告はディスプレイ302に表示される。アクセスログやセキュリティ管理情報はハードディスク等の記憶装置303に記憶され、比較が必要になった時点で読み出される。また、アクセスが行われるたびにセキュリティ管理情報が更新され、記憶装置303に記録される。

【0060】〔第2の実施の形態〕本方式では、通常でないアクセスと判断した場合には警告を発するが、そのアクセスが正当ユーザからのアクセスであると確認できた場合には、アクセスを許可したほうがよい。また、システムの運用上、警告を発した後にアクセスを許可するのか禁止するのかといった選択ができるほうが望ましい。そこで、第2の実施の形態では、このような場合のために、警告処理の手順をいくつか決めておき、それを選択することができるようになっている。

【0061】図13は、本発明の第2の実施の形態についての構成例を示すブロック図である。図13に示すセキュリティ監視装置400は、図2に示すセキュリティ監視装置100と同様の手段を備え、さらに警告処理設定部410と警告処理部420とを備える。なお、警告処理設定部410と警告処理部420以外の図13に示す各手段は、図2に示す同じ番号が付されている手段に対応している。ただし、異常警告部120における警告発信部122は、出力装置140に警告を出力する代わりに、警告処理部420に対して警告を通知する。

【0062】警告処理設定部410は、警告を発した後

に行う警告処理を設定する手段であり、警告処理部420は、異常警告部120からの警告の通知を受けて警告処理設定部410で設定された情報に従って警告処理を行う手段である。

【0063】警告処理設定部410により、予め設定される警告処理設定の例を、図14に示す。また、図15は、各警告処理設定に対応したユーザに対する警告の例、図16は、各警告処理設定に対応した管理者に対する警告の例を示す。

10 【0064】図14に示す(1)の警告処理設定が行われた場合、警告処理部420によって警告が発せられた後、ユーザのアクセスは禁止され、ユーザはロックアウトされる。このとき、ユーザに対して、図15(1)の「このアクセスは禁止されています。あなたのユーザIDはロックされました。再度アクセスするには管理者に連絡してください。」というメッセージが出力される。また、管理者に対しては、図16(1)の「禁止されたアクセスがありました。ユーザxxxxはロックアウトされました。」というメッセージが出力される。

20 【0065】また、図14に示す(2)の警告処理設定が行われた場合、警告処理部420によって警告が発せられた後、ユーザのアクセスは禁止される。このとき、ユーザに対しては、図15(2)のメッセージが出力され、管理者に対しては、図16(2)のメッセージが出力される。

30 【0066】図14に示す(3)の警告処理設定が行われた場合、警告処理部420によって警告が発せられた後、ユーザのアクセスは管理者の許可が出るまで禁止される。ユーザはそれまで待機する。このとき、ユーザに対しては、図15(3)のメッセージが出力され、管理者に対しては、図16(3)のメッセージが出力される。

【0067】図14に示す(4)の警告処理設定が行われた場合、警告処理部420によって警告が発せられた後、ユーザは第2のパスワードが求められ、それが正当と認められる場合に限り、アクセスが許可される。このとき、ユーザに対しては、図15(4)のメッセージが出力され、管理者に対しては、図16(4)のメッセージが出力される。

40 【0068】図14に示す(5)の警告処理設定が行われた場合、警告処理部420によって警告が発せられるが、アクセスは許可される。このとき、ユーザに対しては、図15(5)のメッセージが出力され、管理者に対しては、図16(5)のメッセージが出力される。

【0069】図14に示す(6)の警告処理設定が行われた場合、警告処理部420による警告は行われず、通常通りアクセスが続行される。これは「セキュリティなし」の状態と同じであり、ユーザに対する警告メッセージも管理者に対する警告メッセージも出力されない。

50 【0070】なお、以上の各警告処理設定に応じた警告

メッセージは、管理者だけに出力して、ユーザに対しては何も出さないようにすることも可能である。図17に、第2の実施の形態による処理の流れの概要を示す。アクセスログ取得部111によりアクセスログ201を取得し、セキュリティ管理情報203に変換してセキュリティ管理部112に記録する(ステップS21)。次に、ログ比較部115により、アクセスログ201とセキュリティ管理情報203とを比較し(ステップS22)、アクセスログ201の内容がセキュリティ管理情報203の範囲内であるかどうかにより、通常アクセスかどうかを判断する(ステップS23)。通常アクセスでない場合には、ステップS26へ進み、異常警告部120を介して警告処理部420による警告処理を行う。通常アクセスである場合には、さらに、制限比較部116によりアクセスログ201とアクセス制限情報204とを比較し(ステップS24)、アクセスログ201がアクセス制限の範囲内であるかどうかを判断する(ステップS25)。アクセスログ201がアクセス制限情報204に基づくアクセス制限の範囲内であれば、ステップS26へ進む。アクセスログ201がアクセス制限の範囲外であれば、警告処理を行うことなく、次のアクセスを待つ。

【0071】ステップS26では、警告処理設定部410により事前に設定された警告処理設定に従って、図15および図1-6に示すようなメッセージを出力し、図14に示す警告処理を実行する。

【0072】〔第3の実施の形態〕第1および第2の実施の形態では、コンピュータへのアクセスの例について説明したが、本方式は、基本的に住居侵入監視、交通監視などの監視を必要とする機器のすべてに応用できる。

【0073】図18は、本発明の第3の実施の形態についての構成例を示すブロック図である。セキュリティ監視装置500は、カメラ監視部510、異常警告部520、監視カメラ等530、表示装置540を備える。

【0074】監視カメラ等530は、前述した実施の形態におけるコンピュータの入力手段に相当し、カメラ監視部510は、図1に示すアクセス監視手段10に、異常警告部520は異常警告手段20に、表示装置540は出力装置40に、それぞれ相当する。

【0075】図19は、図18に示す装置を住居侵入監視装置として用いる場合の例を示す。住居侵入監視に関しては、家人の帰宅時間、人数、できれば顔画像などの情報を取得しておき、通常とは異なる時間帯や人が来訪した際に警告を発する。

【0076】具体的には、家人の帰宅時間、人数、できれば顔画像などの画像情報を監視カメラ等530から画像・音声入力部511によって取得し、画像・音声ログ管理部512に記憶する。さらに、画像・音声比較部515により、画像・音声ログ管理部512に記憶したこれまでの来訪者等の情報と比較し、通常とは異なる来訪

であると判断した場合には、異常警告部520により、表示装置540に警告メッセージを表示し、またはブザー等を用いて警告する。さらに、制限比較部516により、予め設定したアクセス制限情報をもとに、禁止されている来訪者または来訪時間等の来訪であるかを調べて警告を発することもできる。なお、画像を入力する例を説明したが、マイクロホンから入力した音声情報をセキュリティチェックに用いることもできる。

【0077】図20は、図18に示す装置を交通監視装置として用いる場合の例を示す。交通監視では、例えば交差点などのある地点を通る車の情報、ナンバー、車種、運転手などを取得し、指定された車以外の車が通行した際に警告を発する。

【0078】具体的には、ある地点の通過車の情報、ナンバー、車種、運転手などを監視カメラ等530から画像・音声入力部511により取得し、画像・音声ログ管理部512に記憶する。さらに、画像・音声比較部515により、画像・音声ログ管理部512に記憶したこれまでの通過車等の情報と比較し、通常とは異なる通過車であると判断した場合には、異常警告部520により、表示装置540に警告メッセージを表示し、またはブザー等を用いて警告する。さらに、制限比較部516により、予め設定したアクセス制限情報をもとに、通過が禁止されている車または運転者等であるかを調べて警告を発することもできる。

【0079】図21は、第3の実施の形態による処理の流れの概要を示す。監視カメラ等530から画像・音声情報を入力し、画像・音声ログ管理部512に記憶する(ステップS31)、画像・音声比較部515は、入力した画像・音声情報と画像・音声ログ管理部512が記憶する画像・音声ログ管理情報とを比較する(ステップS32)。画像・音声ログ管理情報の中に、入力した画像・音声情報と一致するものがあるかどうかを判断し(ステップS33)、一致するものがなければ、異常警告部520により警告を発する(ステップS36)。画像・音声ログ管理情報に一致するものがある場合には、さらに、制限比較部516によりアクセス制限情報と比較し(ステップS34)、画像・音声アクセス制限情報の範囲内であるかどうかを判断する(ステップS35)。画像・音声情報がアクセス制限情報の範囲内であれば、異常警告部520により警告を発する(ステップS36)。

【0080】以上のように、本方式により、

- 1) アクセス内容に応じたセキュリティ管理情報を保存でき、
- 2) ログ比較処理で用いる基準を、アクセス頻度、アクセス内容(書き込み、読み込み、実行など)に応じて任意に設定でき、
- 3) アクセス制限情報のアクセス指定期間を無期限に設定することなどにより、アクセス禁止を設定すること

ができ、

4) セキュリティレベルを管理するため、複数のセキュリティ管理情報ファイルを設けて、時間経過やアクセス回数などのユーザのアクセス時間経過に応じて使用するセキュリティ管理情報ファイルを変更し、セキュリティレベルを変更管理することができ、

5) 警告が発せられた後、アクセスをどのように許可するか等の警告処理を設定することができるようになる。

【0081】したがって、より強固かつ適切なセキュリティ管理を行うことができるようになる。

【0082】

【発明の効果】以上説明したとおり、本発明によれば、ユーザの認証に基づくセキュリティの維持、管理方式によらず、ユーザやネットワークからのアクセス状況を監視し、通常の状態と異なる状態のアクセスを検出することによって、もしユーザの認証情報が漏洩したような場合であっても不正と考えられるアクセスを検出することができ、強固なセキュリティの維持管理を行うことが可能になる。

【図面の簡単な説明】

【図1】本発明の概要を説明するための図である。

【図2】本発明の第1の実施の形態についての構成例を示すブロック図である。

【図3】アクセスログの例を示す図である。

【図4】ユーザに関するセキュリティ管理情報の例を示す図である。

【図5】コンピュータに関するセキュリティ管理情報の例を示す図である。

【図6】あるユーザのアクセス時刻の分布の例を示す図である。

【図7】アクセス制限情報の例を示す図である。

【図8】新規ユーザに対するアクセス制限情報の例を示す図である。

【図9】ネットワーク経由のアクセスから得られるアクセスログの例を示す図である。

【図10】ネットワーク経由のアクセスから得られるア

クセスログのセキュリティ管理情報の例を示す図である。

【図11】第1の実施の形態による処理の流れの概要を示す図である。

【図12】第1の実施の形態において本発明を実現するハードウェアの構成例を示す図である。

【図13】本発明の第2の実施の形態についての構成例を示すブロック図である。

【図14】警告処理設定の例を示す図である。

10 【図15】警告処理設定に応じたユーザに対する警告の例を示す図である。

【図16】警告処理設定に応じた管理者に対する警告の例を示す図である。

【図17】第2の実施の形態による処理の流れの概要を示す図である。

【図18】本発明の第3の実施の形態についての構成例を示すブロック図である。

【図19】図18に示すセキュリティ監視装置を住居侵入監視装置として用いる場合の例を示す図である。

20 【図20】図18に示すセキュリティ監視装置を交通監視装置として用いる場合の例を示す図である。

【図21】第3の実施の形態による処理の流れの概要を示す図である。

【符号の説明】

1 セキュリティ監視装置

2 電子機器

10 アクセス監視手段

11 アクセスログ取得手段

12 セキュリティ管理手段

13 アクセス制限設定手段

14 セキュリティチェック手段

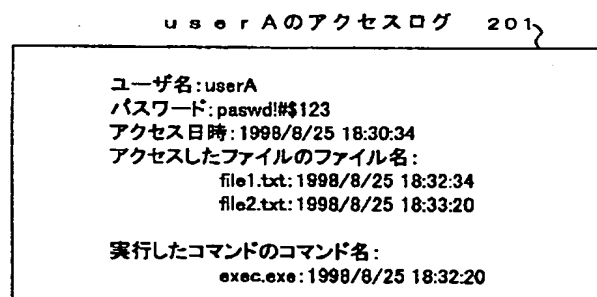
20 異常警告手段

30 警告処理手段

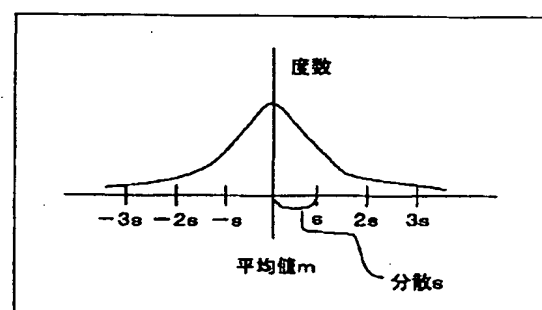
31 警告処理設定手段

40 出力装置

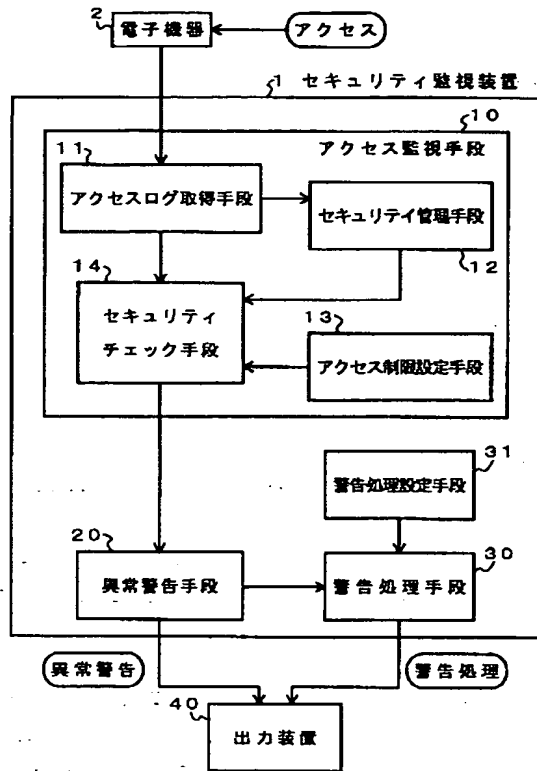
【図3】



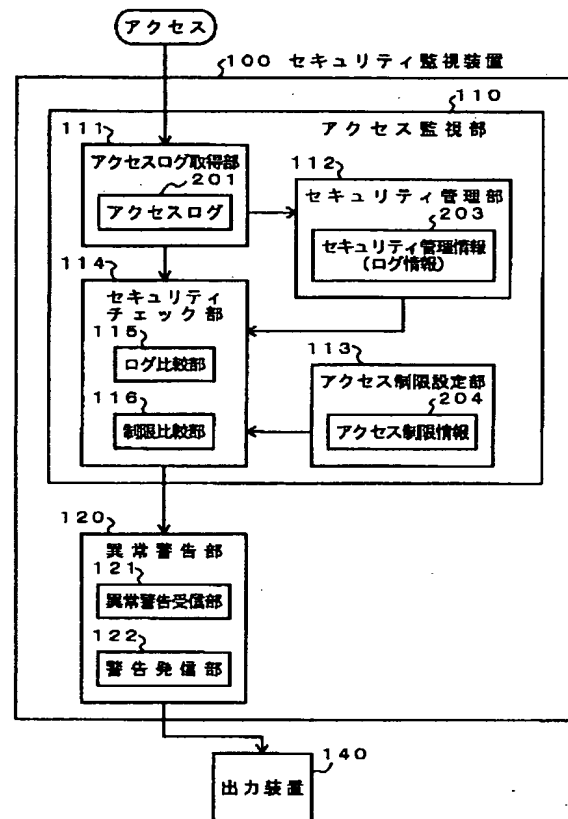
【図6】



【図 1】



【図 2】



【図 4】

セキュリティ管理情報 203

```

ユーザ名: userA
パスワード: paswd!#$123
アクセス回数: 123
アクセス日時: 初回: 1997/8/25 10:30:34、前回: 1998/8/24 10:32:34、時間帯: 10:00:00~ 19:00:00
アクセスしたファイル:
  file1.txt: 初回: 1997/8/25 12:32:34、前回: 1998/8/25 17:30:34、頻度: 22、時間帯: 12:00:00 ~ 17:30:34
  file2.txt: 初回: 1997/8/30 10:32:34、前回: 1998/8/25 17:32:34、頻度: 12、時間帯: 10:00:00 ~ 17:32:34
  execo.exe: 初回: 1997/8/30 10:32:34、前回: 1998/8/25 18:32:20、頻度: 62、時間帯: 10:00:00 ~ 19:30:34
  ...
実行したコマンド
  execo.exe: 初回: 1997/8/30 10:32:34、前回: 1998/8/25 18:32:20、頻度: 62、時間帯: 10:00:00 ~ 19:30:34
  com.exe: 初回: 1997/8/31 10:32:34、前回: 1998/8/25 18:22:20、頻度: 105、時間帯: 10:00:00 ~ 19:30:34
  ...
アクセスするコンピュータ:
  comp1, comp2, comp3
  ...

```

【図 5】

セキュリティ管理情報 203

コンピュータ名: compB
 登録ユーザ: userA, userB, ...
 アクセスファイル:
 file1.txt: 初回: 1995/8/25 12:32:34, 前回: 1998/8/25 17:30:34, 頻度: 222, 時間帯: 12:00:00 - 17:30:34
 file2.txt: 初回: 1997/8/30 10:32:34, 前回: 1998/8/25 17:32:34, 頻度: 122, 時間帯: 10:00:00 - 17:32:34
 exec.exe: 初回: 1998/5/31 10:32:34, 前回: 1998/8/27 15:22:50, 頻度: 305, 時間帯: 10:00:00 - 15:30:34
 ...
 実行コマンド
 exec.exe: 初回: 1995/8/30 10:32:34, 前回: 1998/8/25 18:32:20, 頻度: 642, 時間帯: 10:00:00 - 19:30:34
 comexe: 初回: 1998/5/31 10:32:34, 前回: 1998/8/27 15:22:50, 頻度: 305, 時間帯: 10:00:00 - 15:30:34
 ...
 アクセスするコンピュータ:
 comp1: 初回: 1995/3/30 15:22:34, 前回: 1998/8/22 15:32:20, 頻度: 542, 時間帯: 15:00:00 - 18:00:00
 comp2: 初回: 1995/4/3 15:32:23, 前回: 1998/8/25 18:32:20, 頻度: 542, 時間帯: 15:00:00 - 19:00:34
 ...
 アクセスされたコンピュータ:
 comp1: 初回: 1995/3/30 15:32:34, 前回: 1998/8/20 15:32:20, 頻度: 542, 時間帯: 15:00:00 - 17:00:34
 comp2: 初回: 1996/5/20 20:32:35, 前回: 1998/8/25 18:32:20, 頻度: 344, 時間帯: 18:00:00 - 22:30:34
 server1: 初回: 1995/8/20 8:32:54, 前回: 1998/8/27 8:32:20, 頻度: 632, 時間帯: 4:00:00 - 9:00:14
 server2:
 ...

【図 7】

アクセス制限情報 204

ユーザ名: userA
 アクセスファイル設定:
 file1.txt: 頻度3以下、時間帯9:00:00 - 18:00:00以外
 file2.txt: 頻度3以下、時間帯9:00:00 - 18:00:00以外
 file3.txt: 時間帯0:00:00 - 0:00:00以外
 コマンド実行設定:
 exec.exe: 頻度3以下、時間帯9:00:00 - 18:00:00以外
 cmd.exe: 頻度-1以下、時間帯0:00:00 - 0:00:00以外

【図 8】

アクセス制限情報 (新規ユーザ用) 205

ユーザ名: new
 アクセスファイル設定:
 file1.txt: 頻度0以下、時間帯9:00:00 - 18:00:00以外
 file2.txt: 頻度0以下、時間帯9:00:00 - 18:00:00以外
 file3.txt: 時間帯0:00:00 - 0:00:00以外
 コマンド実行設定:
 exec.exe: 頻度0以下、時間帯9:00:00 - 18:00:00以外
 cmd.exe: 頻度-1以下、時間帯0:00:00 - 0:00:00以外

【図 9】

ネットワーク経由のアクセスログ 206

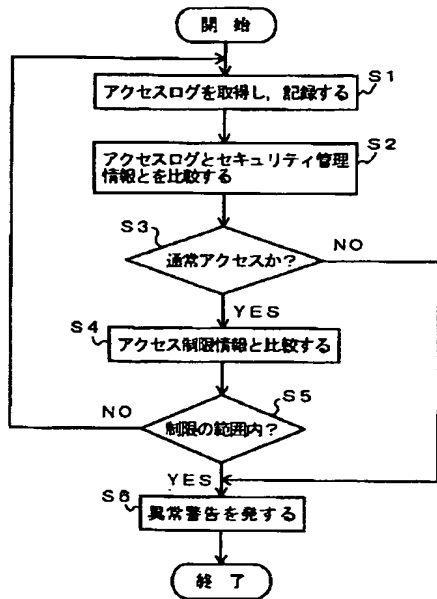
接続してきたコンピュータ名: mailserv1
 メールの宛先: userA
 メールの送信者: senderX
 経由したコンピュータ名: mailserv2, mailserv3
 メールの受信日時: 1998/3/20 14:22:36
 使用プロトコル: smtp

【図 10】

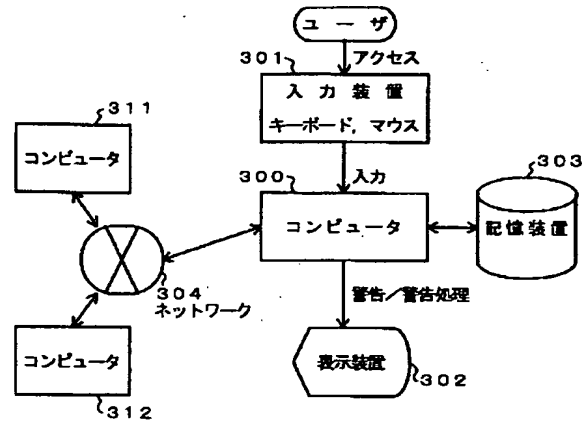
セキュリティ管理情報 207

接続してきたコンピュータ名: mailserv1, mailserv2, ...
 メールの宛先: userA, userB, ...
 メールの送信者: senderX, senderY, senderZ, ...
 経由したコンピュータ名: mailserv2, mailserv3
 メールの受信日時: 1998/3/20 14:22:36
 使用プロトコル: smtp, ...

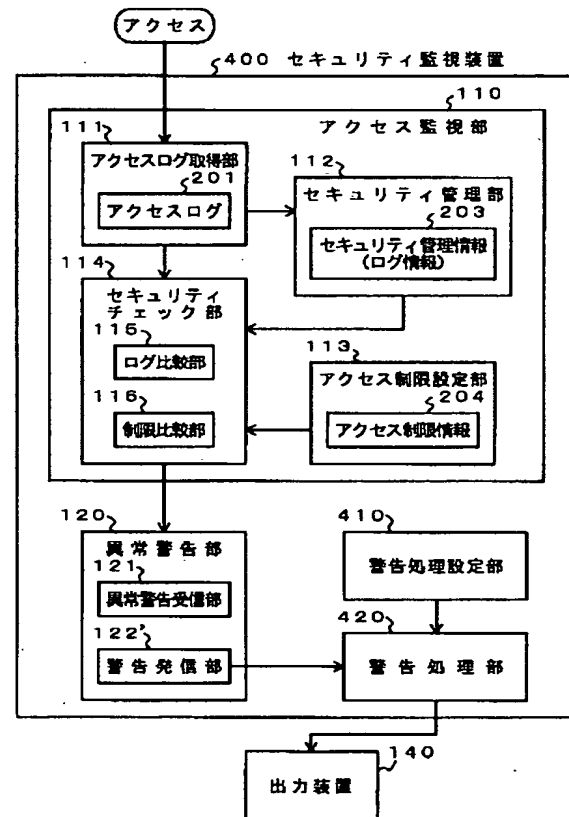
【図 11】



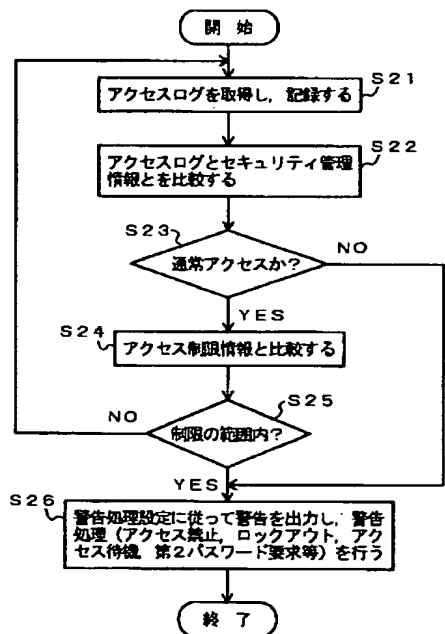
【図 12】



【図 13】



【図 17】



【図 14】

警告処理設定の例

(1)	警告を発し、アクセスを禁止し、ユーザをロックアウトする
(2)	警告を発し、アクセスを禁止する
(3)	警告を発し、管理者が許可するまでアクセスを禁止する。ユーザをそれまで待機させる。
(4)	警告を発し、ユーザに第2のパスワードを求め、それが正当と認められる場合に限り、アクセスを許可する
(5)	警告を発するのみで、アクセスは認める
(6)	通常どおりアクセスを認める

【図 15】

ユーザに対する警告の例

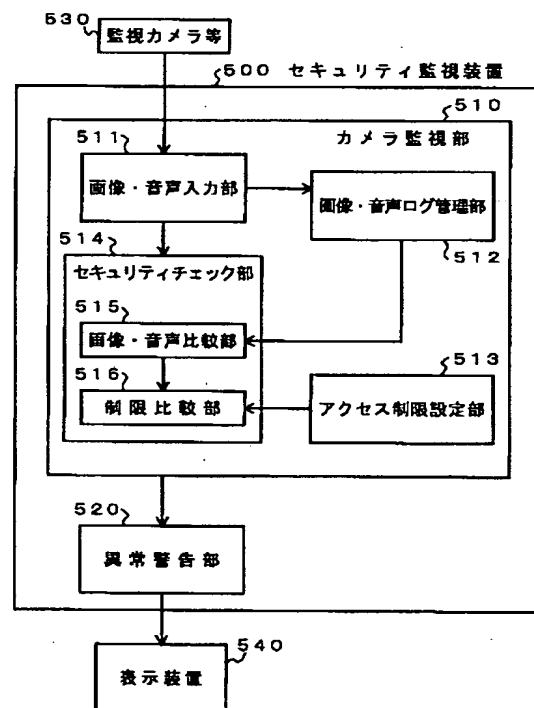
(1)	このアクセスは禁止されています。あなたのユーザIDはロックされました。再度アクセスするには管理者に連絡してください
(2)	このアクセスは禁止されています。
(3)	このアクセスは制限されています。管理者の許可が得るまで、このままお待ちください。
(4)	このアクセスは制限されています。第2パスワードを入力してください
(5)	このアクセスは通常アクセスではありませんが、アクセスは許可します。
(6)	警告なし

【図 16】

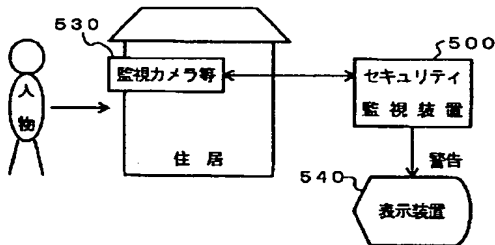
管理者に対する警告の例

(1)	禁止されたアクセスがありました。ユーザ×××××はロックアウトされました。
(2)	禁止されたアクセスがありました。ユーザ：00000
(3)	制限されたアクセスがあります。このアクセスを許可しますか？
(4)	制限されたアクセスがありました。第2パスワードを要求しました
(5)	制限されたアクセスがありました。
(6)	警告なし

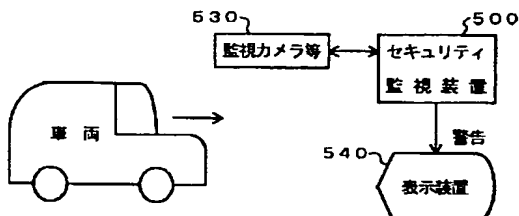
【図 18】



【図 19】



【図 20】



【図 21】

